

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-115241

(43)Date of publication of application : 02.05.1997

(51)Int.Cl. G11B 20/10
G11B 7/00

(21)Application number : 08-105568

(71)Applicant : SONY CORP

(22)Date of filing : 25.04.1996

(72)Inventor : SAKO YOICHIRO
KURIHARA AKIRA
OSAWA YOSHITOMO
KAWASHIMA ISAO
OWA HIDEO

(30)Priority

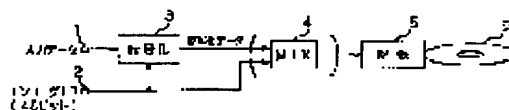
Priority number : 07166644 Priority date : 30.06.1995 Priority country : JP
07206085 11.08.1995 JP

(54) DEVICE AND METHOD FOR RECORDING DATA, DEVICE AND METHOD FOR REPRODUCING DATA, AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To make it possible to know production history of a recording medium and to prevent a copy from being performed easily by providing an input means for receiving specific identification information and a recording means recording at least the identification information on the recording medium.

SOLUTION: This device is provided with a cyphering circuit 3 cyphering the input data to be recorded based on an encoder ID, and records the data cyphered by the circuit 3 on an optical disk D together with the encoder ID. A mixer circuit 4 is provided on the prestage of a recording means 5, and the encoder ID is mixed in the data sequence of the cyphered data in the circuit 4. Thus, the encoder ID is recorded on the data recording area of the disk D on which the cyphered data is to be recorded. By recording the encoder ID on the disk D, the history of a data recorder is stored in the disk D. Further, because, the history is able to be pursued, somebody who tries to copy the disk, will give up to copy the disk, and an illicit copy is prevented.



LEGAL STATUS

[Date of request for examination] 20.04.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-115241

(43) 公開日 平成9年(1997)5月2日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
G 1 1 B 20/10		7736-5D	G 1 1 B 20/10	H
7/00		9464-5D	7/00	Q

審査請求 未請求 請求項の数69 O L (全 16 頁)

(21) 出願番号 特願平8-105568

(22) 出願日 平成8年(1996)4月25日

(31) 優先権主張番号 特願平7-166644

(32) 優先日 平7(1995)6月30日

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平7-206085

(32) 優先日 平7(1995)8月11日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 佐古 曜一郎

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 栗原 章

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 大澤 義知

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 弁理士 小池 晃 (外2名)

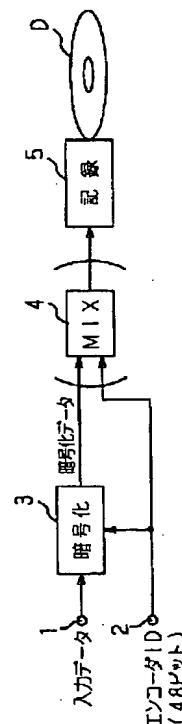
最終頁に続く

(54) 【発明の名称】 データ記録装置及び方法、データ再生装置及び方法、並びに記録媒体

(57) 【要約】

【課題】 情報が簡単に複製されることなく、また、複製されたとしても再生できない。

【解決手段】 データ記録装置固有のエンコーダIDが入力される端子2と、少なくともエンコーダIDを光ディスクDに記録する記録手段5と、端子1を介して供給される記録すべき入力データをエンコーダIDに基づいて暗号化する暗号化回路3とを有し、エンコーダIDと共に暗号化データを光ディスクDに記録する。



【特許請求の範囲】

【請求項1】 記録媒体にデータを記録するデータ記録装置において、

固有の識別情報が入力される入力手段と、

少なくとも上記識別情報を記録媒体に記録する記録手段とを有することを特徴とするデータ記録装置。

【請求項2】 上記識別情報は、データ記録装置固有の識別情報であることを特徴とする請求項1記載のデータ記録装置。

【請求項3】 上記記録手段は、上記識別情報を記録媒体の所定の領域に記録することを特徴とする請求項1記載のデータ記録装置。

【請求項4】 記録媒体に記録すべきデータのデータ列に上記識別情報を混在させる混在手段を備え、

上記記録手段は、上記記録すべきデータと共に当該データ列に混在した上記識別情報を上記記録媒体に記録することを特徴とする請求項1記載のデータ記録装置。

【請求項5】 記録媒体に記録すべきデータを上記識別情報に基づいて暗号化する暗号化手段を備え、

上記記録手段は、上記識別情報と共に上記暗号化されたデータを上記記録媒体に記録することを特徴とする請求項1記載のデータ記録装置。

【請求項6】 上記記録手段は、上記識別情報を記録媒体の所定の領域に記録することを特徴とする請求項5記載のデータ記録装置。

【請求項7】 上記暗号化されたデータのデータ列に上記識別情報を混在させる混在手段を備え、

上記記録手段は、上記暗号化されたデータと共に当該データ列に混在した上記識別情報を上記記録媒体に記録することを特徴とする請求項5記載のデータ記録装置。

【請求項8】 データ記録装置によって記録媒体にデータを記録する際のデータ記録方法において、

データ記録装置固有の識別情報を入力し、

少なくとも上記識別情報を記録媒体に記録することを特徴とするデータ記録方法。

【請求項9】 上記識別情報を記録媒体の所定の領域に記録することを特徴とする請求項8記載のデータ記録方法。

【請求項10】 記録媒体に記録すべきデータのデータ列に上記識別情報を混在させて、上記記録すべきデータと共に記録することを特徴とする請求項8記載のデータ記録方法。

【請求項11】 記録媒体に記録すべきデータを上記識別情報に基づいて暗号化し、

上記識別情報と共に上記暗号化されたデータを記録媒体に記録することを特徴とする請求項8記載のデータ記録方法。

【請求項12】 上記識別情報を記録媒体の所定の領域に記録することを特徴とする請求項11記載のデータ記

録方法。

【請求項13】 上記暗号化されたデータのデータ列に上記識別情報を混在させ、上記暗号化されたデータと共に記録することを特徴とする請求項11記載のデータ記録方法。

【請求項14】 データ記録装置によってデータが記録される記録媒体において、

データ記録装置固有の識別情報を少なくとも記録してなることを特徴とする記録媒体。

【請求項15】 所定の領域に上記識別情報を記録してなることを特徴とする請求項14記載の記録媒体。

【請求項16】 上記識別情報を混在したデータを記録してなることを特徴とする請求項14記載の記録媒体。

【請求項17】 上記識別情報と共に、当該識別情報に基づいて暗号化された暗号化データを記録してなることを特徴とする請求項14記載の記録媒体。

【請求項18】 所定の領域に上記識別情報を記録してなることを特徴とする請求項17記載の記録媒体。

【請求項19】 上記識別情報を混在した上記暗号化されたデータを記録してなることを特徴とする請求項17記載の記録媒体。

【請求項20】 記録データと共にデータ記録装置固有の識別情報を少なくとも記録してなる記録媒体からデータを再生するデータ再生装置であって、

上記記録媒体からデータを読み取るデータ読み取り手段と、

上記記録媒体から読み取られたデータより上記識別情報を抽出する識別情報抽出手段とを有し、

上記識別情報を抽出できないときには上記記録媒体からのデータの再生を停止することを特徴とするデータ再生装置。

【請求項21】 上記データ読み取り手段は、記録媒体の所定の領域に記録されている上記識別情報を読み取ることを特徴とする請求項20記載のデータ再生装置。

【請求項22】 上記識別情報抽出手段は、上記記録媒体から読み取られたデータのデータ列に混在する上記識別情報を抽出することを特徴とする請求項20記載のデータ再生装置。

【請求項23】 上記識別情報に基づいて暗号化されている上記記録データの当該暗号化を、上記識別情報抽出手段により抽出した識別情報に基づいて解く暗号化解除手段を設けることを特徴とする請求項20記載のデータ再生装置。

【請求項24】 上記データ読み取り手段は、記録媒体の所定の領域に記録されている上記識別情報を読み取ることを特徴とする請求項23記載のデータ再生装置。

【請求項25】 上記識別情報抽出手段は、上記記録媒体から読み取られた上記暗号化されている記録データのデータ列に混在する上記識別情報を抽出することを特徴とする請求項23記載のデータ再生装置。

【請求項26】 記録データと共にデータ記録装置固有の識別情報を少なくとも記録してなる記録媒体からデータを再生するデータ再生装置であって、上記記録媒体からデータを読み取るデータ読み取り手段と、

上記記録媒体から読み取られたデータより上記識別情報を抽出する識別情報抽出手段と、
上記識別情報に基づいて暗号化されている記録データの当該暗号化を、上記識別情報抽出手段により抽出した識別情報に基づいて解く暗号解除手段と、を有することを特徴とするデータ再生装置。

【請求項27】 上記データ読み取り手段は、記録媒体の所定の領域に記録されている上記識別情報を読み取ることを特徴とする請求項26記載のデータ再生装置。

【請求項28】 上記識別情報抽出手段は、上記記録媒体から読み取られた上記暗号化されている記録データのデータ列に混在する上記識別情報を抽出することを特徴とする請求項27記載のデータ再生装置。

【請求項29】 記録データと共にデータ記録装置固有の識別情報を少なくとも記録してなる記録媒体からデータを再生するデータ再生方法であって、
上記記録媒体からデータを読み取り、
上記記録媒体から読み取られたデータより上記識別情報を抽出し、
上記識別情報を抽出できないときには上記記録媒体からのデータの再生を停止することを特徴とするデータ再生方法。

【請求項30】 記録媒体の所定の領域に記録されている上記識別情報を読み取ることを特徴とする請求項29記載のデータ再生方法。

【請求項31】 上記記録媒体から読み取られたデータのデータ列に混在する上記識別情報を抽出することを特徴とする請求項29記載のデータ再生方法。

【請求項32】 上記識別情報に基づいて暗号化されている上記記録データの当該暗号化を、上記抽出した識別情報に基づいて解くことを特徴とする請求項29記載のデータ再生方法。

【請求項33】 記録媒体の所定の領域に記録されている上記識別情報を読み取ることを特徴とする請求項32記載のデータ再生方法。

【請求項34】 上記記録媒体から読み取られた上記暗号化されている記録データのデータ列に混在する上記識別情報を抽出することを特徴とする請求項32記載のデータ再生方法。

【請求項35】 記録データと共にデータ記録装置固有の識別情報を少なくとも記録してなる記録媒体からデータを再生するデータ再生方法であって、
上記記録媒体からデータを読み取るデータ読み取り、
上記記録媒体から読み取られたデータより上記識別情報を抽出し、

上記識別情報に基づいて暗号化されている記録データの当該暗号化を、上記抽出した識別情報に基づいて解くことを特徴とするデータ再生方法。

【請求項36】 記録媒体の所定の領域に記録されている上記識別情報を読み取ることを特徴とする請求項35記載のデータ再生方法。

【請求項37】 上記記録媒体から読み取られた上記暗号化されている記録データのデータ列に混在する上記識別情報を抽出することを特徴とする請求項35記載のデータ再生方法。

【請求項38】 情報提供側と情報収集側との間を結ぶ情報伝達手段と、

上記情報伝達手段を通じて情報提供側と情報収集側との間で情報を送受信するための送受信手段と、
情報提供側が情報収集側に暗号化された情報を配信するための情報媒体と、

情報収集側から送信された当該情報収集側の持つ少なくとも一つ以上の固有情報を利用して、上記情報媒体の上記暗号化された情報の解読に必要な鍵情報を暗号化する鍵暗号化手段と、

情報提供側から送信された上記暗号化された鍵情報を、
上記固有情報を利用して解読する暗号鍵解読手段と、
上記情報媒体の情報を読み取る情報媒体読み取り手段と、

上記解読した鍵情報を用いて、上記情報媒体から読み取った上記暗号化された情報を解読する暗号情報解読手段とを具備することを特徴とする情報提供収集装置。

【請求項39】 上記情報提供側は、上記情報収集側から送信された、上記情報媒体を特定する媒体識別情報と、当該情報媒体内の情報を特定する情報識別情報とを用いて、課金処理を行うことを特徴とする請求項38記載の情報提供収集装置。

【請求項40】 上記情報収集側の持つ少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化手段を設け、

上記情報提供側に送信する上記媒体識別情報及び情報識別情報を、当該情報暗号手段により暗号化することを特徴とする請求項39記載の情報提供収集装置。

【請求項41】 上記情報収集側の持つ少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化手段と、

上記情報媒体から読み取った情報を蓄積する情報蓄積手段とを設け、

上記情報媒体から読み取り、上記暗号情報解読手段にて暗号を解読した情報を上記情報蓄積手段に蓄積する際には、上記暗号を解読した情報を上記情報暗号化手段にて暗号化してから蓄積することを特徴とする請求項38記載の情報提供収集装置。

【請求項42】 上記暗号情報解読手段は、上記固有情報に基づいて生成した鍵情報を用いて、上記情報蓄積手

段に蓄積した暗号化された情報を解読することを特徴とする請求項41記載の情報提供収集装置。

【請求項43】 上記情報収集側の持つ少なくとも一つ以上の固有情報は、情報媒体毎に各々異なる固有の情報を除く情報であることを特徴とする請求項38記載の情報提供収集装置。

【請求項44】 情報伝達手段を通じて情報提供側との間で情報を送受信するための送受信手段と、情報提供側より配信され暗号化された情報を有してなる情報媒体から、情報を読み取る情報媒体読み取り手段と、上記送受信手段を介して送信した少なくとも一つ以上の固有情報を利用して情報提供側にて暗号化され、上記送受信手段を介して受信した鍵情報を、上記固有情報に基づいて解読する暗号鍵解読手段と、上記解読した鍵情報を用いて、上記情報媒体から読み取った上記暗号化された情報を解読する暗号情報解読手段と、を具備することを特徴とする情報収集装置。

【請求項45】 上記情報媒体を特定する媒体識別情報と、当該情報媒体内の情報を特定する情報識別情報とを上記情報提供側に送信することを特徴とする請求項44記載の情報収集装置。

【請求項46】 上記少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化手段を設け、上記情報提供側に送信する上記媒体識別情報及び情報識別情報を、当該情報暗号手段により暗号化することを特徴とする請求項45記載の情報収集装置。

【請求項47】 上記少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化手段と、上記情報媒体から読み取った情報を蓄積する情報蓄積手段とを設け、上記情報媒体から読み取り、上記暗号情報解読手段にて暗号を解読した情報を上記情報蓄積手段に蓄積する際には、上記暗号を解読した情報を上記情報暗号化手段にて暗号化してから蓄積することを特徴とする請求項44記載の情報収集装置。

【請求項48】 上記暗号情報解読手段は、上記固有情報に基づいて生成した鍵情報を用いて、上記情報蓄積手段に蓄積した暗号化された情報を解読することを特徴とする請求項47記載の情報収集装置。

【請求項49】 上記少なくとも一つ以上の固有情報は、情報媒体毎に各々異なる固有の情報を除く情報であることを特徴とする請求項44記載の情報収集装置。

【請求項50】 情報伝達手段を通じて情報収集側との間で情報を送受信するための送受信手段と、情報収集側から送信される当該情報収集側の持つ少なくとも一つ以上の固有情報を利用して、上記情報収集側に配信した暗号化された情報を有してなる情報媒体の、当該暗号化された情報の解読に必要な鍵情報を暗号化する鍵暗号化手段とを具備することを特徴とする情報提供装置。

【請求項51】 上記情報収集側から送信されてくる上記情報媒体を特定する媒体識別情報と、当該情報媒体内の情報を特定する情報識別情報とを用いて、課金処理を行うことを特徴とする請求項50記載の情報提供装置。

【請求項52】 上記情報収集側の持つ少なくとも一つ以上の固有情報を用いて暗号化された上記媒体識別情報及び情報識別情報を、上記情報収集側から送信されてくる上記固有情報を用いて解読する暗号情報解読手段を備えることを特徴とする請求項51記載の情報提供装置。

【請求項53】 上記情報収集側の持つ少なくとも一つ以上の固有情報は、情報媒体毎に各々異なる固有の情報を除く情報であることを特徴とする請求項50記載の情報提供装置。

【請求項54】 情報提供側と情報収集側との間を結ぶ情報伝達工程と、

上記情報伝達工程を通じて情報提供側と情報収集側との間で情報を送受信する送受信工程と、

情報提供側により配信され暗号化された情報を有してなる情報媒体から、情報を読み取る情報媒体読み取り工程と、

情報収集側から送信された当該情報収集側の持つ少なくとも一つ以上の固有情報を利用して、上記情報媒体の上記暗号化された情報の解読に必要な鍵情報を暗号化する鍵暗号化工程と、

情報提供側から送信された上記暗号化された鍵情報を、上記固有情報を利用して解読する暗号鍵解読工程と、上記解読した鍵情報を用いて、上記情報媒体から読み取った上記暗号化された情報を解読する暗号情報解読工程とを有することを特徴とする情報提供収集方法。

【請求項55】 上記情報提供側は、上記情報収集側から送信された、上記情報媒体を特定する媒体識別情報と、当該情報媒体内の情報を特定する情報識別情報とを用いて、課金処理を行うことを特徴とする請求項54記載の情報提供収集方法。

【請求項56】 上記情報収集側の持つ少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化工程を設け、

上記情報提供側に送信する上記媒体識別情報及び情報識別情報を、当該情報暗号工程により暗号化することを特徴とする請求項55記載の情報提供収集方法。

【請求項57】 上記情報収集側の持つ少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化工程と、

上記情報媒体から読み取った情報を蓄積する情報蓄積工程とを設け、

上記情報媒体から読み取り、上記暗号情報解読工程にて暗号を解読した情報を上記情報蓄積工程にて蓄積する際には、上記暗号を解読した情報を上記情報暗号化工程にて暗号化してから蓄積することを特徴とする請求項54記載の情報提供収集方法。

【請求項58】 上記暗号情報解読工程では、上記固有情報に基づいて生成した鍵情報を用いて、上記情報蓄積工程にて蓄積した暗号化された情報を解読することを特徴とする請求項57記載の情報提供収集方法。

【請求項59】 上記情報収集側の持つ少なくとも一つ以上の固有情報は、情報媒体毎に各々異なる固有の情報を除く情報であることを特徴とする請求項54記載の情報提供収集方法。

【請求項60】 情報伝達手段を通じて情報提供側との間で情報を送受信するための送受信工程と、情報提供側より配信され暗号化された情報が記録されてなる情報媒体から、情報を読み取る情報媒体読み取り工程と、

上記送受信工程を介して送信した少なくとも一つ以上の固有情報を利用して情報提供側にて暗号化され、上記送受信工程を介して受信した鍵情報を、上記固有情報に基づいて解読する暗号鍵解読工程と、

上記解読した鍵情報を用いて、上記情報媒体から読み取った上記暗号化された情報を解読する暗号情報解読工程と、を有することを特徴とする情報収集方法。

【請求項61】 上記情報媒体を特定する媒体識別情報と、当該情報媒体内の情報を特定する情報識別情報とを上記情報提供側に送信することを特徴とする請求項60記載の情報収集方法。

【請求項62】 上記少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化工程を設け、

上記情報提供側に送信する上記媒体識別情報及び情報識別情報を、当該情報暗号工程により暗号化することを特徴とする請求項61記載の情報収集方法。

【請求項63】 上記少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化工程と、

上記情報媒体から読み取った情報を蓄積する情報蓄積工程とを設け、

上記情報媒体から読み取り、上記暗号情報解読工程にて暗号を解読した情報を上記情報蓄積工程にて蓄積する際には、上記暗号を解読した情報を上記情報暗号化工程にて暗号化してから蓄積することを特徴とする請求項60記載の情報収集方法。

【請求項64】 上記暗号情報解読工程では、上記固有情報に基づいて生成した鍵情報を用いて、上記情報蓄積工程にて蓄積した暗号化された情報を解読することを特徴とする請求項63記載の情報収集方法。

【請求項65】 上記少なくとも一つ以上の固有情報は、情報媒体毎に各々異なる固有の情報を除く情報であることを特徴とする請求項60記載の情報収集方法。

【請求項66】 情報伝達手段を通じて情報収集側との間で情報を送受信するための送受信工程と、情報収集側から送信される当該情報収集側の持つ少なくとも一つ以上の固有情報を利用して、上記情報収集側に配信した暗号化された情報を有してなる情報媒体の、当

該暗号化された情報の解読に必要な鍵情報を暗号化する鍵暗号化工程とを具備することを特徴とする情報提供方法。

【請求項67】 上記情報収集側から送信されてくる上記情報媒体を特定する媒体識別情報と、当該情報媒体内の情報を特定する情報識別情報とを用いて、課金処理を行うことを特徴とする請求項66記載の情報提供方法。

【請求項68】 上記情報収集側の持つ少なくとも一つ以上の固有情報を用いて暗号化された上記媒体識別情報及び情報識別情報を、上記情報収集側から送信されてくる上記固有情報を用いて解読する暗号情報解読工程を備えることを特徴とする請求項67記載の情報提供方法。

【請求項69】 上記情報収集側の持つ少なくとも一つ以上の固有情報は、情報媒体毎に各々異なる固有の情報を除く情報であることを特徴とする請求項66記載の情報提供方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、記録媒体にデータを記録するデータ記録装置及び方法、記録媒体に記録されているデータを再生するデータ再生装置及び方法、並びにデータが記録されてなる記録媒体に関し、また本発明は、例えばテキスト情報と共に映像や音楽等のいわゆるマルチメディア情報或いはプログラム情報を提供し、収集する情報提供／収集装置及び方法に関する。

【0002】

【従来の技術】 音声や各種データ等の情報信号が記録されるデータ記録媒体として、近年は、これら情報信号を光学的に記録するもの、具体的には音楽用のいわゆるコンパクトディスク（CD）や当該CD規格のディスクをデータ用に使用するCD-ROM等が、全世界に普及している。

【0003】 また、従来より、情報提供サービスは、例えば電話回線などを用いて利用者端末（情報収集側の端末）と情報提供者とを結び、利用者の所望する情報を取り出す、いわゆるデータベースシステムやパソコン通信システムとして実現されている。また、情報提供サービスとしては、暗号化した情報を記録したいわゆるCD-ROMなどの大容量メディアを配布すると共に、上記暗号化された情報を復号するための鍵情報を例えば通信を介して利用者に送ることにより、当該CD-ROM内に記録されている暗号化された情報を復号させ、この復号した情報をハードディスク等に複写して利用するようなサービスも出現している。

【0004】 さらに、特公平2-60007号公報には、ファイルキーを暗号キーで暗号化したパスワードをコンピュータに入力し、記憶媒体に書き込まれたプログラムを暗号機構で解読するようにして、ソフトウェアプログラムの複製及び共有化を防止する技術が開示されている。

【0005】

【発明が解決しようとする課題】ところで、上述のようなCDやCD-ROM等に記録された情報の全てを再生装置で読み取って例えばハードディスク等にコピーし、その後、当該ハードディスクにコピーしたデータを、CDやCD-ROM等のエンコードシステムに供給して新たにCDやCD-ROMを作成することで、元のCDやCD-ROMと全く同じ海賊版を容易に作成することができるという具合に、従来はコピープロテクションなどのセキュリティ機能が充分ではなかった。

【0006】また、上述の問題は、次世代のデータ記録媒体と言われているいわゆるデジタルビデオディスク(DVD)でも深刻である。

【0007】一方、従来の情報提供サービスの方法では、暗号を解くための鍵情報を利用者に伝送する際に、鍵情報そのものを例えば音声を使って電話で伝送するようなことが行われており、特に当該鍵情報に対する暗号化が行われることはなかった。このような鍵情報の伝送方法は、セキュリティの面から不安が大きい。

【0008】また、鍵情報の伝送に通信を利用する場合は、通常1対1の接続なので、この鍵情報が盗まれる危険性は少ないが、鍵情報の伝送にネットワークを利用するような場合には、鍵情報の保護に問題がある。

【0009】したがって、例えば、暗号化された情報が多量に記録されているメディアを情報提供者が配布し、利用者がこのメディアから必要な情報を所望する場合にのみ、暗号を復号するための鍵情報を伝送すると共に課金を行うような情報提供システムにおいても、上述したように鍵情報の伝送の際におけるセキュリティ面での問題があると、鍵情報が実際の利用者以外の者に知られてしまう虞れがあり、この場合、上記情報提供システム自体が成り立たなくなってしまう。また、利用者が正規の利用者かどうか特定できないと、課金が他人に行われたりしてしまう虞れもあり、やはり情報提供システムが成り立たなくなってしまう。

【0010】このようなことから、情報提供者から利用者への鍵情報の伝送のセキュリティをいかに高めるかということ、及び利用者の特定をいかに確実に実行できるようにすることが重要な問題となっている。

【0011】そこで、本発明は上述の実情に鑑み、簡単に複製されることなく、また、複製されたとしても再生できないデータ記録装置及び方法、データ再生装置及び方法、並びに記録媒体を提供するものである。

【0012】また、本発明の他の目的は、情報提供者から利用者への鍵情報の伝送のセキュリティを高めることができると共に、利用者の特定をも確実に実行することができる情報提供／収集装置及び方法を提供することである。

【0013】

【課題を解決するための手段】本発明のデータ記録装置

及び方法は、記録媒体にデータを記録するデータ記録装置及び方法であり、固有の識別情報が入力され、少なくとも上記識別情報を記録媒体に記録することにより、上述の課題を解決する。この識別情報としては、データ記録装置固有の識別情報が挙げられる。

【0014】また、本発明の記録媒体は、データ記録装置によってデータが記録される記録媒体であり、データ記録装置固有の識別情報を少なくとも記録してなることにより、上述の課題を解決する。

【0015】本発明のデータ再生装置及び方法は、記録データと共にデータ記録装置固有の識別情報を少なくとも記録してなる記録媒体からデータを再生するデータ再生装置及び方法であり、上記記録媒体からデータを読み取り、上記記録媒体から読み取られたデータより上記識別情報を抽出し、上記識別情報を抽出できないときには上記記録媒体からのデータの再生を停止することにより、上述の課題を解決する。

【0016】さらに、本発明のデータ再生装置及び方法は、記録データと共にデータ記録装置固有の識別情報を少なくとも記録してなる記録媒体からデータを再生するデータ再生装置及び方法であり、上記記録媒体からデータを読み取るデータ読み取り、上記記録媒体から読み取られたデータより上記識別情報を抽出し、上記識別情報に基づいて暗号化されている記録データの当該暗号化を、上記抽出した識別情報に基づいて解くことにより、上述の課題を解決する。

【0017】以上の構成によれば、データ記録装置固有の識別情報を記録媒体に記録することで、この識別情報を見れば、記録媒体の作成履歴を知ることができる。また、識別情報がないときには記録媒体からのデータの再生を停止することにより、記録媒体からのデータのコピーを防止する。

【0018】また、本発明の情報提供／収集装置及び方法は、情報収集側に暗号化された情報を有してなる情報媒体を情報提供側から配信し、情報提供側と情報収集側との間を情報伝達手段により結び、この情報伝達手段を通じて情報提供側と情報収集側とで情報を送受信し、情報提供側にて情報収集側の持つ少なくとも一つ以上の固有情報を利用して情報媒体の暗号化された情報の解読に必要な鍵情報を暗号化し、情報収集側にて情報提供側から送信された上記暗号化された鍵情報を固有情報を利用して解読し、さらに情報収集側にて上記情報媒体から読み取った暗号化された情報を上記解読した鍵情報を用いて解読することにより、上述した課題を解決する。

【0019】すなわち、本発明によれば、暗号化された情報を有してなる記録媒体から情報を読み出す際には、当該暗号を解読するための鍵情報が必要であるが、この鍵情報は情報提供側が有しており、情報収集側はこの鍵情報の配送を要求するようにし、この際に、鍵情報の受信を受ける情報収集側から情報提供側に当該情報収集側

を特定する固有情報を送り、情報提供側は受信した固有情報から情報収集側を特定すると共に課金処理を行う。同時にこの個別情報を利用して暗号解読用の鍵情報を暗号化してから情報収集側に伝送することで、鍵情報の伝送におけるセキュリティ能力を高めるようにしている。また、情報収集側では受信した暗号化された鍵情報を固有情報により解読し、情報の解読用の鍵情報を取り出し、この鍵情報を用いて情報媒体の暗号化されている情報の解読を行う。

【0020】

【発明の実施の形態】以下、本発明の好ましい実施の形態について、図面を参照にしながら説明する。

【0021】本発明のデータ記録方法を実現する実施の形態のデータ記録装置は、基本構成として、図1に示すように、当該データ記録装置固有の識別情報（以下、エンコードIDと呼ぶ）が入力される端子2と、少なくとも上記エンコードIDを光ディスクDに記録する記録手段5とを有するものである。

【0022】さらに、本実施の形態のデータ記録装置においては、端子1を介して供給される記録すべき入力データを、上記エンコードIDに基づいて暗号化する暗号化回路3を有し、上記エンコードIDと共に上記暗号化回路3によって暗号化されたデータ（以下、暗号化データと呼ぶ）を光ディスクDに記録するようにしている。

【0023】なお、上記エンコードIDは、上記光ディスクDの所定の領域、例えば後述するTOC（table of contents）エリアやヘッダ領域等に記録することができる。或いは、図1に示すように、本実施の形態のデータ記録装置の例えば記録手段5の前段にミックス回路4を設け、当該ミックス回路4において上記暗号化データのデータ列に上記エンコードIDを混在させることにより、当該エンコードIDを上記暗号化データが記録されるべき光ディスクDのデータ記録領域に記録することも可能である。もちろん、記録すべきデータを暗号化しない場合も、上記ミックス回路4において記録データのデータ列にエンコードIDを混在させて、光ディスクDに記録することも可能である。

【0024】上述のように、光ディスクDに対してエンコードIDを記録することで、当該ディスクDにはデータ記録装置の履歴を残すことが可能となる。すなわち、データ記録装置固有の履歴を残すことができれば、例えば違法に作成されたディスクのエンコードIDを見れば、いずれの装置で当該ディスクが作成されたかを知ることができる。また、このように履歴が追えることを周知させるようにすれば、ディスクをコピーすることを思いとどまらせて、違法な複製を未然に防ぐことも可能となる。

【0025】一方、本発明のデータ再生方法が適用される実施の形態のデータ再生装置は、図2に示すように、上記本発明のデータ記録装置によって記録データと共に

エンコードIDが少なくとも記録されている光ディスクDからデータを再生するものであり、上記光ディスクDからデータを読み取るデータ読み取り手段6と、上記光ディスクDから読み取られたデータより上記エンコードIDを抽出する分離回路7とを有するものである。

【0026】ただし、上記エンコードIDが上記光ディスクDの前記所定の領域に記録されているときには、上記データ読み取り手段6自身がエンコードIDの抽出手段として動作し、上記記録データとは別に上記所定領域からエンコードIDを読み取ることになるため、上記分離回路7は必ずしも必要ない。これに対して、上記エンコードIDが記録データのデータ列に混在されているときには、上記データ読み取り手段6にて光ディスクDのデータ領域から上記記録データとエンコードIDとが共に読み出されることになるため、この場合には分離回路7にて上記記録データのデータ列からエンコードIDが抽出される。

【0027】上記記録データとエンコードIDは、復号化回路8に送られることになるが、このとき、当該復号化回路8では、上記エンコードIDが供給されたときには、上記記録データを再生データとして端子9から出力し、一方、エンコードIDが供給されないとき（エンコードIDの認証がないとき）には上記記録データの再生（復号化）を停止する。

【0028】また、上記エンコードIDと共に光ディスクDに記録されているデータが、前記暗号化データであるとき、上記復号化回路8では、上記光ディスクDから読み取られたエンコードIDに基づいて、同じく光ディスクDから読み取られた暗号化データの当該暗号化を解く。すなわち、これは、記録データだけをコピーできたとしても、エンコードIDがなければ暗号化データの当該暗号化を解くことができないことを意味する。このようにして暗号化が解かれたデータが端子9から再生データとして取り出される。

【0029】このように、本実施の形態のデータ再生装置によれば、記録データがコピーされたとしても、エンコードIDの認証がなければ再生データを得ることができないので、セキュリティも高くなる。

【0030】なお、前記光ディスクDは、例えば図3に示すように、中央にセンタ孔102を有しており、この光ディスクDの内周から外周に向かって、プログラム管理領域であるTOC（table of contents）エリアとなるリードイン（lead in）領域103と、データが記録されるデータ領域104と、データ終了領域、いわゆるリードアウト（lead out）領域105とが形成されるものである。ここで、上記エンコードIDを記録データとは別の所定領域に記録する場合には、例えばリードイン領域103等のデータ領域104以外の領域に記録することになる。また、記録データに混在させてエンコードIDを記録する場合には、データ領域104に記録され

ることになる。

【0031】また、前述した実施の形態におけるデータ記録装置としては、例えばオーディオデータやビデオデータ、或いはプログラムデータ等に誤り訂正符号を付加したり変調したりするエンコーダ或いはフォーマッタや、いわゆるカッティング装置、マスタリング装置、スタンピング装置等が考えられ、上記エンコーダIDはこれら装置固有の識別情報となる。さらに、光ディスクDが光磁気ディスク（MOディスク）や、レコーダブルのCD（いわゆるCD-R）である場合、上記エンコーダIDはこれらディスクの記録再生装置固有の識別情報となる。

【0032】次に、上述した光ディスクDを再生するデータ再生装置の概略構成について、図4を用いて説明する。この図4の説明では、記録データがエンコーダIDに基づいて暗号化されており、さらに当該エンコーダIDが暗号化データのデータ列に混在されて記録されている場合の動作について述べる。

【0033】この図4において、光ピックアップ17は、上記光ディスクD上にレーザ光を集光し、このレーザ光の反射光を受光することにより、当該光ディスクDに記録されているデータ信号を読み出し、このデータ信号をデコード回路15に送る。また、光ピックアップ17は、上記レーザ光の反射光に基づくフォーカスサーボエラー信号、トラッキングエラー信号をサーボ回路14に送る。

【0034】サーボ回路14は、コントローラCPU10の制御に基づき、上記フォーカスサーボエラー信号、トラッキングエラー信号に応じたフォーカスサーボ信号及びトラッキングサーボ信号を生成して光ピックアップ17に送る。また、当該サーボ回路14からは、光ディスクDの回転サーボ信号も出力され、モータ18は当該回転サーボ信号により回転が制御される。

【0035】一方、デコード回路15では、上記光ピックアップ17からのデータ信号の復調及び誤り訂正処理を行う。

【0036】ここで、上記光ディスクDのデータ記録領域104から読み出され、上記デコード回路15によりデコードされたデータは、先ず、例えばセクタ単位でエンコーダID抽出回路19に送られる。当該エンコーダID抽出回路19は、上記セクタ単位のデータから、上記エンコーダIDのデータを抽出する。この抽出されたエンコーダIDのデータは、コントローラCPU10により制御されるワークRAM12に蓄えられる。

【0037】このとき、コントローラCPU10は、上記エンコーダIDのデータが抽出された残りの暗号化データを、上記RAM12に蓄えられたエンコーダIDのデータを用いて復号化する。なお、上記コントローラCPU10が使用するプログラムデータはプログラムROM13に蓄えられている。

【0038】上述のようにして復号化された再生データは、インターフェイス回路16を介して出力端子11から外部に出力される。

【0039】上記図4のデータ再生装置における動作の流れは図5に示すようなものとなる。

【0040】この図5において、ステップS1で光ディスクDの読み取りが開始されると、次のステップS2では光ディスクDからセクタ毎にデータが読み出される。

【0041】次のステップS3では、前記エンコーダID抽出回路19により、当該セクタ毎のデータからエンコーダIDのデータが抽出される。

【0042】ステップS4では上記エンコーダIDのデータが抽出された残りの暗号化データを読み出し、ステップS5ではコントロールCPU10にて上記暗号化データをエンコーダIDに基づいて復号化する。

【0043】その後、ステップS6では、上記復号化したデータを再生データとしてインターフェイス回路16に送る。

【0044】次のステップS7では、光ディスクDの再生が終了したか否かの判定を行い、いまだ再生が終了していないと判定したときにはステップS1に戻って上述の処理を行い、再生が終了したときには処理を終了する。

【0045】次に、本発明に係る情報提供及び／又は収集方法の実施の形態について、図面を参照しながら説明する。

【0046】本発明の情報提供／収集方法が適用される情報提供／収集装置、すなわち情報提供システムとしては、図6に示すように、情報収集側の利用者端末400と情報提供者側の情報提供装置200とが、情報伝達手段としての電話回線やローカルエリアネットワーク（LAN）などの通信網300によって結ばれた状況を想定している。

【0047】ここで、上記情報提供システムにおける情報提供装置200は、図7に示すように、利用者側に送出する情報及び当該送出情報を暗号化するための鍵情報を蓄積する情報蓄積装置201と、利用者毎の課金情報及び利用者の電話番号及び利用者の固有番号の情報を蓄積する情報蓄積装置202と、送出情報を上記鍵情報に基づいて暗号化する暗号化回路203と、送出情報を回線に送出できるように変換する変換器204と、通信網（通信回線）300に情報を送出するための通信回線インターフェイス部206と、当該装置200の制御プログラム及びシステムの構成情報を記憶したROM209と、上記制御プログラムを実行するCPU207と、CPU207の一時的な作業情報を記憶しておくためのRAM208と、データバス、アドレスバス、制御バスなどよりなるCPU207のシステムバス210とから構成されている。

【0048】また、利用者端末400の構成は、図8に

示すように、一時的に情報を記憶しておくRAM411と、例えばハードディスクや光磁気ディスク等の少なくとも情報を保存しておくことができる情報蓄積装置412と、情報蓄積装置412から読み出した情報を表示するための表示信号を生成する表示回路413と、表示回路413からの表示信号に基づいた表示を行う表示装置414と、当該端末400を操作するための例えばキーボードやマウス等の操作装置415と、情報提供装置200からの暗号化情報を解読する暗号解読回路416と、情報提供者により配布された情報記録媒体を読み出す情報媒体読み取り装置417と、情報媒体読み取り装置417固有の識別番号(ID)情報を保持するROM418と、当該端末400の制御プログラム及び端末400の構成情報を記憶したROM420と、制御プログラムを実行するCPU419と、通信網(通信回線)300に情報を送出するための通信回線インターフェイス部421と、データバス、アドレスバス、制御バスなどよりなるCPU419のシステムバス422とから構成されている。

【0049】以下に、上述した情報提供装置200と通信網300と利用者端末400とからなる情報提供システムの動作について、利用者側と情報提供者側との間の通信網300(通信回線)として例えばいわゆるISDN(サービス総合デジタル網)の回線を利用した場合について説明する。

【0050】利用者は、先ず始めに情報提供者が無償或いは有償で配布する大容量の情報蓄積媒体301を入手する。なお、上記情報蓄積媒体301は、例えば光記録媒体であるいわゆるCD-ROMなどの大容量の情報蓄積メディアを使用しており、多量の暗号化された情報が記録されている。その他、当該CD-ROMのような読み出し専用の媒体以外に、ライトワンス或いは光磁気ディスクのような記録可能な媒体を使用することも可能である。またこのとき、当該利用者端末400の読み出し専用メモリのROM418には情報読み取り装置417の固有の識別番号(以下読み取り装置IDと呼ぶ)が記録されており、情報蓄積媒体301には当該媒体を識別するためのID(以下媒体識別IDと呼ぶ)及び当該媒体301内の各々の情報を識別するためにID(以下情報識別IDと呼ぶ)が記録されている。さらに、利用者は個別のID(以下利用者IDと呼ぶ)及びパスワードを持つ。

【0051】このような前提の元、利用者が所望の情報を上記情報蓄積媒体301から読み出す場合の手順を図9～図12を用いて詳細に説明する。

【0052】図9のAの部分には、利用者端末400から情報提供装置200側に送出する情報を記述してある。すなわち、利用者端末400から送出する情報は、利用者の固有の番号情報であり、例えば、電話発番号、利用者ID、パスワード、読み取り装置ID及び情報の

特定に必要な媒体識別ID、情報識別IDからなる。電話発番号は、利用者の電話番号であり、ISDNでは発信者から着信者に向けて電話番号を(発番号)を自動的に送ることができるようになっている。

【0053】先ず、図10を用いて、利用者端末400での動作から説明する。

【0054】この図10において、利用者端末400のCPU419は、ステップS501にて情報記録媒体301が当該端末400の情報媒体読み取り装置417にセットされたか否かの判断を行う。当該ステップS501で情報記録媒体301がセットされていないと判断した場合にはこのステップS501の判断を繰り返し、セットされたと判断した場合にはステップS502に進む。なお、情報記録媒体301を読み取る情報媒体読み取り装置417は、当該情報記録媒体301が着脱可能なものである。

【0055】次に、利用者は、端末400の操作装置415を操作することにより、情報蓄積媒体301内の所望の情報の検索処理を行う。このときのCPU419は、操作装置415からの目次情報表示の指示があるか否かの判定を行い、無いと判定した場合にはステップS502の判定を繰り返し、有ると判定した場合にはステップS503に進む。ステップS503では、利用者による操作装置415の操作に応じて、端末400の情報媒体読み取り装置417にセットした情報記録媒体301から目次情報を再生し、この再生された目次情報に基づく表示信号を表示回路413が生成し、この表示信号を表示装置414に送ることによって表示画面上に上記目次情報が表示される。なお、上記目次情報には、上記情報蓄積媒体301内に記録されている情報の一部内容の閲覧が可能なものも含まれる。

【0056】次のステップS504では、CPU419が上記表示装置414の表示画面上に表示された目次情報の内から上記操作装置415の操作による検索操作がなされているか否かの判断を行い、無いと判断した場合にはステップS504の判断を繰り返し、有ると判断したときにはステップS505に進む。このステップS505では検索中の内容表示が行われる。ステップS506では、CPU419において上記検索表示された内容の内の何れかに対して、利用者から操作装置415を介して情報を取り出す指示が入力されたか否かの判断を行う。このステップS506にて取りだし指示がなされていないと判断したときにはステップS505に戻り、指示されたと判断したときにはステップS507に進む。このステップS507では指定された情報のID情報の読み取りを行う。すなわち、ステップS504～ステップS507までの検索操作においては、利用者が希望する情報を見つけることができたとき、利用者が上記操作装置415を操作することにより、情報蓄積媒体301からその内容を取り出す指示が行われ、当該指示入力

有ったときにはその指定した情報のID情報を該当する情報蓄積媒体301から読み取る。

【0057】次のステップS508では、情報媒体IDを同様にして情報蓄積媒体301から読み取り、ステップS509に進む。

【0058】このステップS509では、CPU419が情報提供者に発呼処理を行う。すなわち、予め設定されている情報提供者の電話番号を情報蓄積装置412から読み出し、通信回線インターフェイス部421に設定する。このとき、ステップS510のように、当該通信回線インターフェイス部421は情報提供者の情報提供装置200に発呼動作を行い回線を接続する。

【0059】次のステップS511では、CPU419が情報提供装置200に送り出す情報を準備し、ステップS512に進む。ここで、上記情報提供装置200に送り出す情報は、情報媒体ID、情報識別ID、利用者ID、パスワード、情報媒体読み取り装置IDである。ステップS512では、CPU419において、これらのうち情報媒体IDと情報識別ID、情報媒体読み取り装置IDに対して、利用者IDとパスワードを用いて暗号化処理を行う。

【0060】その後、ステップS513において、暗号化された情報は、通信回線インターフェイス部21を介して情報提供者の情報提供装置200に送られ、ステップS514にて情報提供装置200からの送信待ち状態となる。

【0061】次に、情報提供者側の処理について説明する。すなわち、図9のBの部分に記述するように、利用者端末400からの発呼があると、情報提供装置200は、媒体識別IDと情報識別IDとから利用者の必要とする情報を特定し、該当する解読鍵情報を、読み取り装置ID、利用者ID、パスワード、電話番号を利用して暗号化して利用者端末400に送信する。

【0062】この処理動作を図11を用いて説明すると、ステップS530では、CPU7は先ず利用者端末400からの送信（発呼）が有るか否かの判断を行っており、無いと判断した場合には待ち状態としてステップS530の判断を繰り返している。このステップS530において、有ると判断した場合にはステップS531に進む。このステップS531では、CPU207が、上記利用者端末400から通信回線を通して供給された前記暗号化された情報を、通信回線インターフェイス部206、変換器204を介して読み込む。

【0063】次のステップS532において、CPU207は、受信した利用者IDを元に、情報蓄積装置202に保存している利用者の課金情報の中にあるパスワードを読み出し、利用者IDと組み合わせて、受信した暗号化情報の解読を行う。次のステップS533では、上記ステップS532での解読の結果、読み出された情報媒体IDと情報識別IDを使って、情報蓄積装置201

に蓄積されている情報媒体管理情報から該当する情報の解読鍵情報を得る。

【0064】ステップS534では、上記得られた解読鍵情報を、利用者ID、パスワード、読み取り装置IDと共に暗号化回路203に送り、ここで暗号化を施した後、ステップS535にて、変換器204、通信回線インターフェイス部206を経て、利用者端末400に送る。すなわち、図9のCに示すように、情報提供装置200から利用者端末400に送られる情報は、暗号化された解読鍵情報である。

【0065】次に、上記情報提供装置200からの暗号化された解読鍵情報を受信した利用者端末400では、図12に示す処理を行う。すなわち、当該暗号化された解読鍵情報を受信した利用者端末400では、図9のDに示すように、固有番号を使って、上記暗号化された解読鍵情報を解読し、この解読した解読鍵情報を利用して情報蓄積媒体301上の暗号化されている情報を解読する。

【0066】図12において、前記ステップS514のように情報提供装置200からの送信待ち状態となっている利用者端末400では、ステップS515にて情報提供装置200からの送信が有ったか否かの判断を行っており、送信が無いときにはこの判断を繰り返し、送信が有ったならばステップS516の処理を行う。

【0067】ステップS516では、CPU419が上記通信回線インターフェイス部421を通して受信した上記暗号化された解読鍵情報を暗号解読回路416に送る。

【0068】当該暗号解読回路416では、ステップS517に示すように、利用者ID、パスワード、情報媒体読み取り装置417の固有番号である読み取り装置IDを、ROM418から受け取り、これらを用いて上記受信した暗号化された解読鍵情報の解読を行う。

【0069】次のステップS518では、上述のようにして暗号解読回路416にて解読された解読鍵情報を用いて、CPU419が情報蓄積媒体301に記録されている、暗号化されている所望の情報を読み出させ、暗号解読回路416に送る。暗号解読回路416では、上記暗号化されている所望の情報の暗号を上記解読鍵情報を用いて解読し、利用者が利用可能な平文情報を得る。

【0070】ステップS519では、上記平文情報を表示回路413に送り、当該表示回路413にて生成された上記平文情報の表示信号を表示装置414に送る。これにより、表示装置414の表示画面上には、利用者が読み取ることができる形の上記平文情報の表示がなされる。

【0071】なお、上述の説明では、表示装置414の表示画面上に平文情報を表示するまでについて述べているが、上記平文化情報を情報蓄積装置412に複写する場合には、当該平文化情報をそのまま情報蓄積装置41

2に複写することは行わず、当該平文化情報を前記CPU419にて情報媒体読み取り装置のIDと利用者のIDにより暗号化してから蓄積記録するものとする。この情報蓄積装置412に蓄積した情報を読み出す場合には、情報蓄積装置412からの上記暗号化された情報を、暗号解読回路416に送り、ここで情報媒体読み取り装置IDと利用者IDを元に情報の解読を行うようにする。また、本構成例では、情報提供者の情報提供装置200と利用者端末400との間を接続する情報伝達手段としてISDN回線を用いた例を説明したが、通常のアナログ電話回線やCATV回線（ケーブルテレビジョン回線）、無線通信回線、LAN（ローカルエリアネットワーク）等を利用した場合も容易に実現可能であることは言うまでもなく、さらには通信回線ではなく郵便や宅配便にて情報の受け渡しを行う場合であっても、本発明は適用できる。

【0072】さらに、上述の例では、利用者の個別の識別情報として利用者IDやパスワードを用いているが、この利用者個別の識別情報としては、利用者端末400の機器番号や、利用者の電話番号、利用者の定めた暗証番号、ネットワークインターフェイスの物理アドレス等を用いることもできる。なお、利用者端末400の機器番号を上記個別の識別情報として用いた場合、暗号解読回路416に当該機器番号情報が直接供給されるように構成することも可能である。

【0073】上述したように、本発明にかかる情報提供システムによれば、多量の情報を大容量の情報記録媒体に纏めて記録したものを利用者に配布し、通信回線やネットワーク等を介して所望の情報についての暗号を解読するための解読鍵情報を伝送するシステムを構築した場合、読み取り装置に固有の番号（ID）にて暗号化した解読鍵情報を情報提供者側から送信するようにすることで、解読鍵情報を万一回線やネットワークから傍受されたとしても、当該傍受者は正しい解読鍵情報を得ることが不可能となるので、セキュリティ能力を向上することが可能となる。

【0074】また、利用者端末から、情報読み取り装置のID等の利用者固有のID情報を暗号化して情報提供装置側に送り、それを元にして情報提供装置側では解読鍵情報を暗号化してから利用者端末側に送るようにしていることも、セキュリティの面から有効である。

【0075】さらに、情報媒体読み取り装置から他の情報蓄積装置に情報を複写する際にも、必ず読み取り装置のIDを使って暗号化してから書き込むようにしているので、違法コピーの防止をすることが可能となる。ここで、読み取り装置のIDは利用者から操作や読み取りが不可能な形で構成することで、さらにセキュリティ能力を高めることが可能である。すなわち、情報蓄積媒体から読み出した情報を利用者端末において複製する場合には、一度暗号を解読した情報をそのまま複製することも

可能であるが、本発明の構成例では、上述したように、一度解読した情報を再度情報読み取り装置のID情報の複数の固有情報で暗号化し直すことで、よりセキュリティ能力を高めるようにしている。

【0076】なお、米国特許第5,392,351号の電子化データ保護方式にて示されるように、情報媒体に予め一意の媒体固有番号と共に暗号化した暗号化電子化データを書き込んでおき、許諾側で媒体の一意の媒体固有番号を元に媒体固有鍵を生成し、この媒体固有鍵によって暗号化電子化データ復号鍵を暗号化し、この暗号化したデータを媒体に許諾情報として書き込み、使用側で媒体から読み込んだ媒体固有番号を元に媒体固有鍵を生成し、媒体から読み込んだ許諾情報をこの媒体固有鍵によって復号して元の電子化データ復号鍵を生成し、この電子化データ復号鍵によって媒体から読み込んだ暗号化電子化データを復号し、平文の電子化データを生成するようなものも存在している。しかし、このような情報媒体毎にそれぞれ異なる固有のID（例えば媒体固有のシリアルナンバ等）を前提にして電子化データ復号鍵を生成するものの場合、CD-ROMのように大量複製される媒体にそれぞれに固有のID情報を記録することは困難である。これに対して、本発明にかかる情報提供システムにおいては、情報蓄積媒体の媒体識別IDはそれぞれの媒体毎に固有のIDである必要はなく、媒体内に記録されている情報も各々の媒体で同一の暗号化処理が行われたものにできるため、大量複製が可能となり、したがってCD-ROMのような媒体に適用可能である。さらに、上記電子化データ保護方式では、許諾側が電子化データ復号鍵を暗号化し、この暗号化した電子化データ復号鍵を許諾情報として媒体に書き込んでから、使用者側に使用させるようにしているので、このことから上記CD-ROMのように大量複製される媒体には不向きであるのに対して、本発明では、解読鍵情報の伝送の際に、利用者から情報読み取り装置IDなど利用者固有のIDを情報提供側に通信回線を介して送出し、情報提供側ではそれを元に解読鍵情報を暗号化して再び通信回線を介して利用者に送り返すようにしているため、大量複製される媒体であっても有効に適用できる。上述のようなことから、本発明によれば、情報記録媒体の製造時に固有の情報を記録しなくてもよいので、製造コストが上昇することなく、安価に製造できることになる。

【0077】

【発明の効果】本発明においては、データ記録装置固有の識別情報を記録媒体に記録することで、この識別情報を見れば、記録媒体の作成履歴を知ることができ、このことから簡単に複製が行われることを防止できる。また、識別情報がないときには記録媒体からのデータの再生を停止することにより、記録媒体からのデータのコピーを防止できる。

【0078】また本発明においては、情報収集側に暗号

化された情報を有してなる情報媒体を情報提供側から配信し、情報提供側と情報収集側との間を情報伝達手段により結び、この情報伝達手段を通じて情報提供側と情報収集側とで情報を送受信し、情報提供側にて情報収集側の持つ少なくとも一つ以上の固有情報を利用して情報媒体の暗号化された情報の解読に必要な鍵情報を暗号化し、情報収集側にて情報提供側から送信された上記暗号化された鍵情報を固有情報を利用して解読し、さらに情報収集側にて上記情報媒体から読み取った暗号化された情報を上記解読した鍵情報を用いて解読することにより、情報提供側から情報収集側への鍵情報の伝送のセキュリティを高めることができると共に、情報収集側の特定をも確実に行うことができる。

【図面の簡単な説明】

【図1】本発明に係る実施の形態のデータ記録装置の基本構成を説明するための図である。

【図2】本発明に係る実施の形態のデータ再生装置の基本構成を説明するための図である。

【図3】本実施の形態の光ディスクの構成について説明するための図である。

【図4】本実施の形態の光ディスクを再生するデータ再生装置の具体的構成を示すブロック回路図である。

【図5】本実施の形態の光ディスクからのデータ再生時の動作の流れを示すフローチャートである。

【図6】本発明にかかる情報提供システムの構成例を示すブロック回路図である。

【図7】情報提供システムの情報提供装置の構成例を示すブロック回路図である。

すブロック回路図である。

【図8】情報提供システムの利用者端末の構成例を示すブロック回路図である。

【図9】情報提供システムでの動作及び伝送される情報について説明するための図である。

【図10】利用者端末から情報提供装置へ暗号化情報を送信するまでの処理の流れを示すフローチャートである。

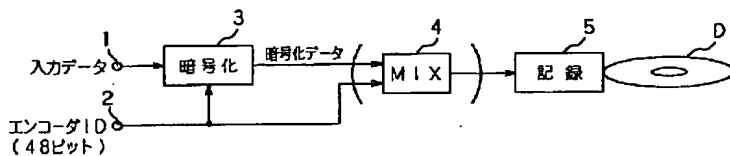
【図11】情報提供装置から利用者端末へ暗号化した解読鍵情報を送信するまでの処理の流れを示すフローチャートである。

【図12】情報提供装置からの暗号化された解読鍵情報を用いて、情報蓄積媒体の暗号化された情報を解読するまでの利用者端末における処理の流れを示すフローチャートである。

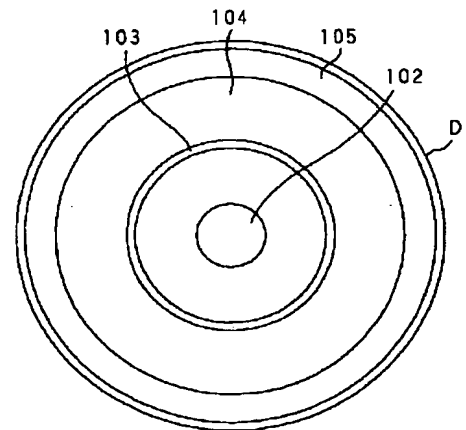
【符号の説明】

3 暗号化回路、 4 ミックス回路、 5 記録手段、 6 データ読み取り手段、 7 分離回路、 8 復号化回路、 D 光ディスク、 201, 202, 412 情報蓄積装置、 203 暗号化回路、 206, 421 通信回線インターフェイス部、 200 情報提供装置、 207, 419 CPU、 300 通信網、 301 情報蓄積媒体、 400 利用者端末、 413 表示回路、 414 表示装置、 415 操作装置、 416 暗号解読回路、 417 情報媒体読み取り装置

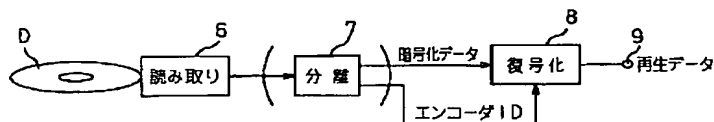
【図1】



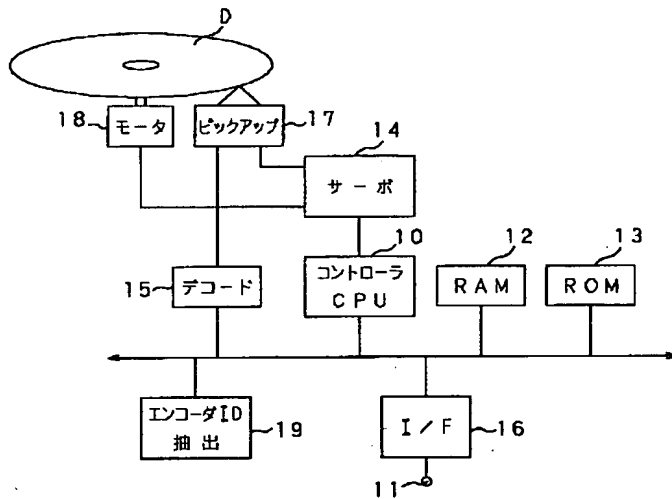
【図3】



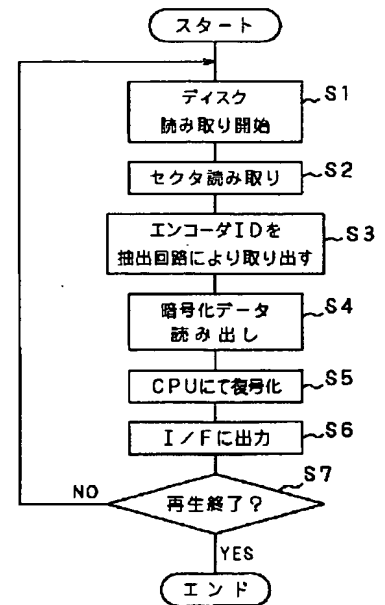
【図2】



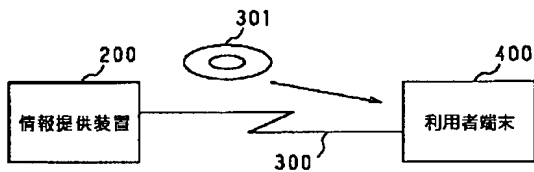
【図4】



【図5】

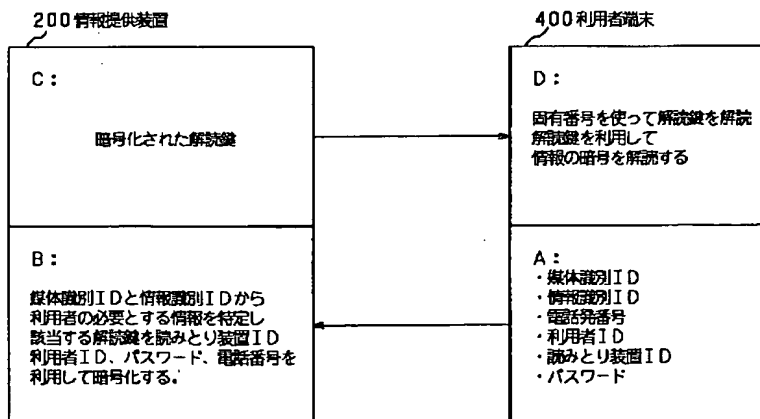


【図6】

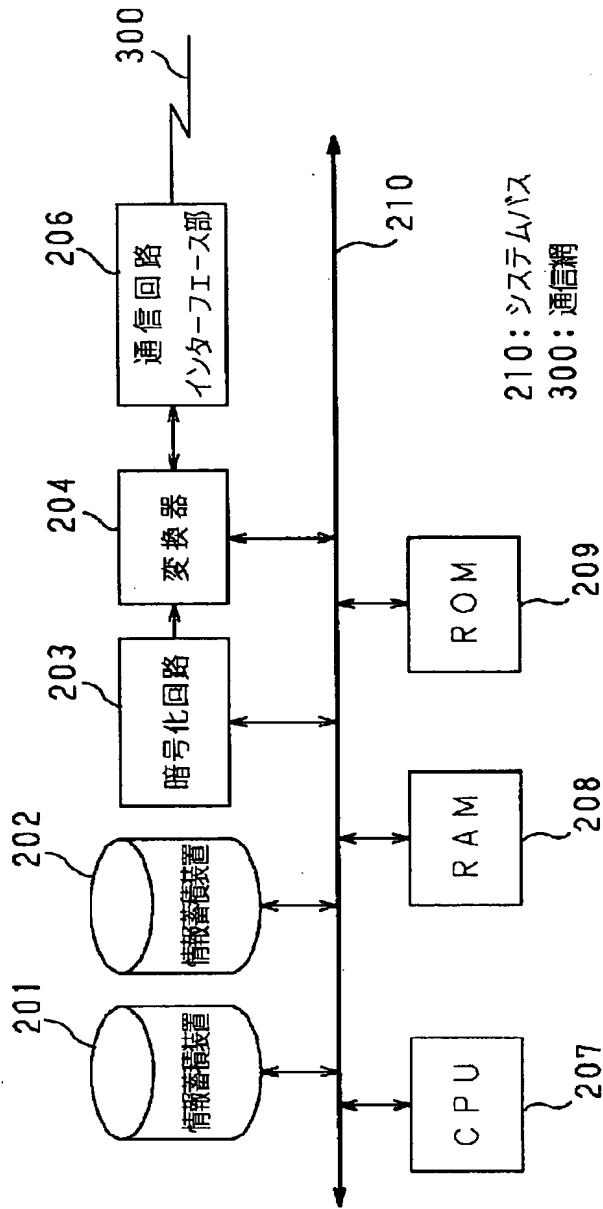


300: 通信網
301: 情報蓄積媒体 (CD-ROM)

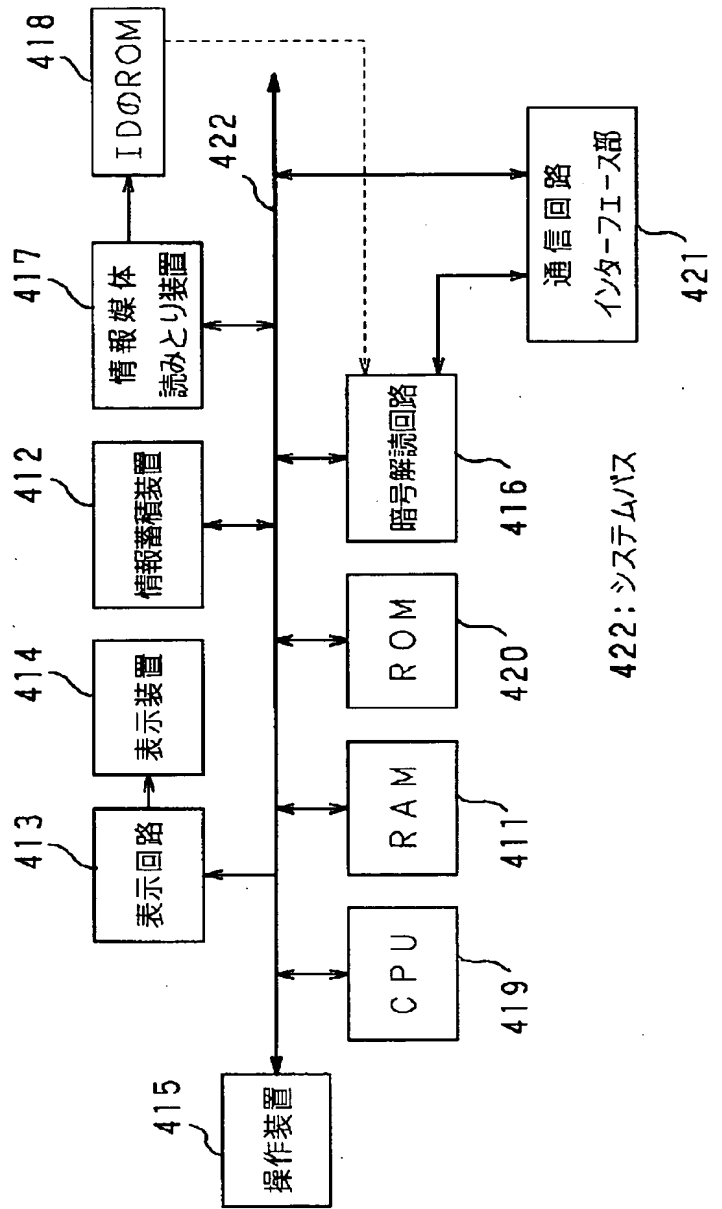
【図9】



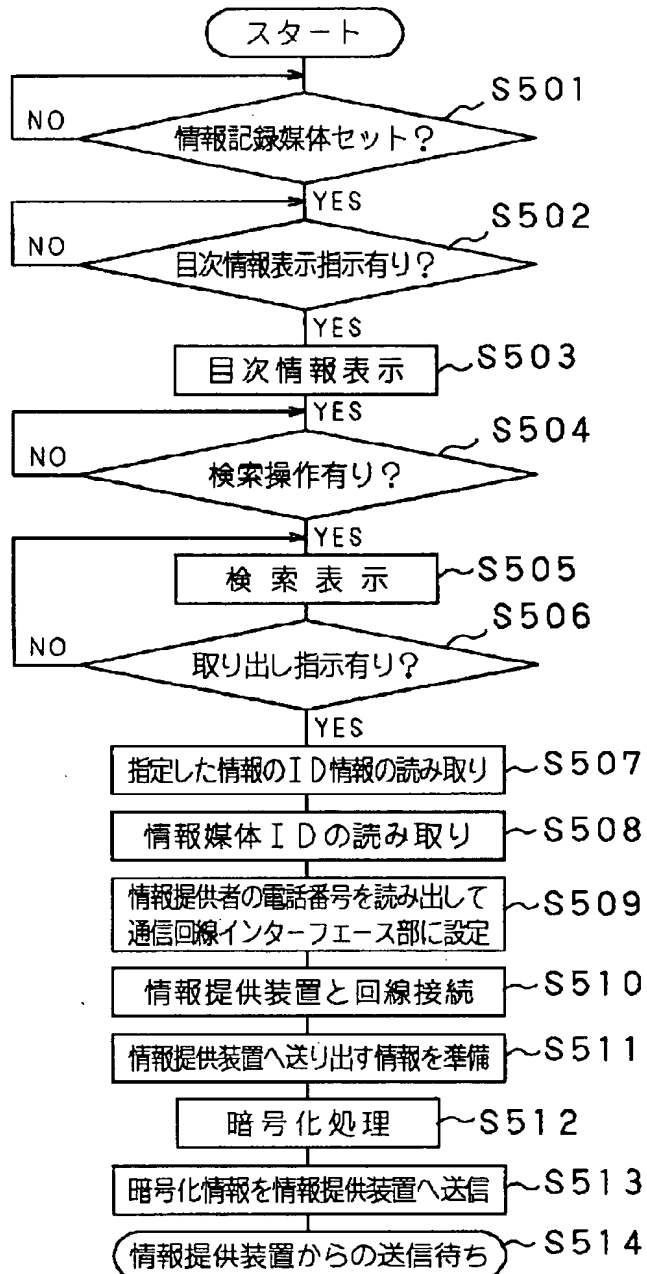
【図7】



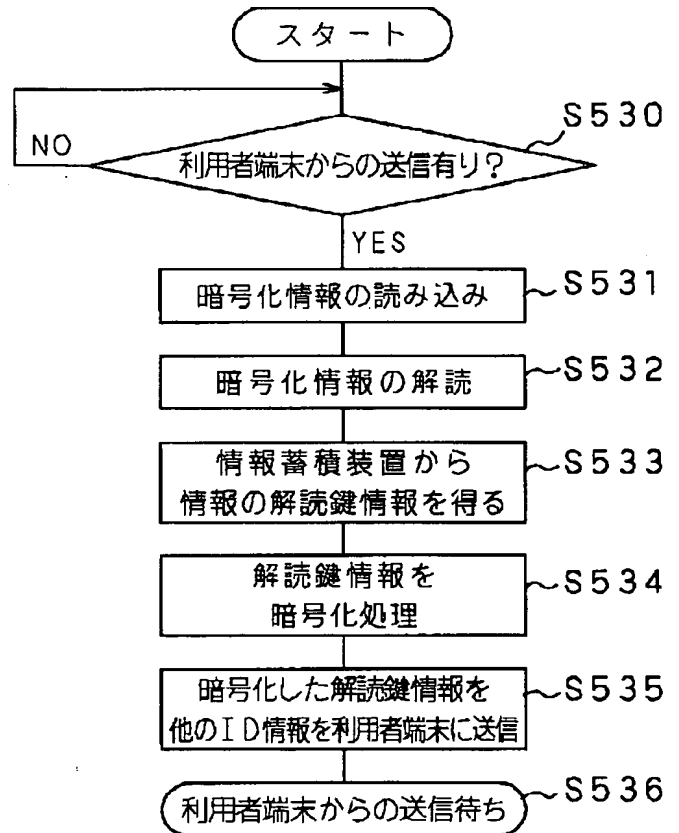
【図8】



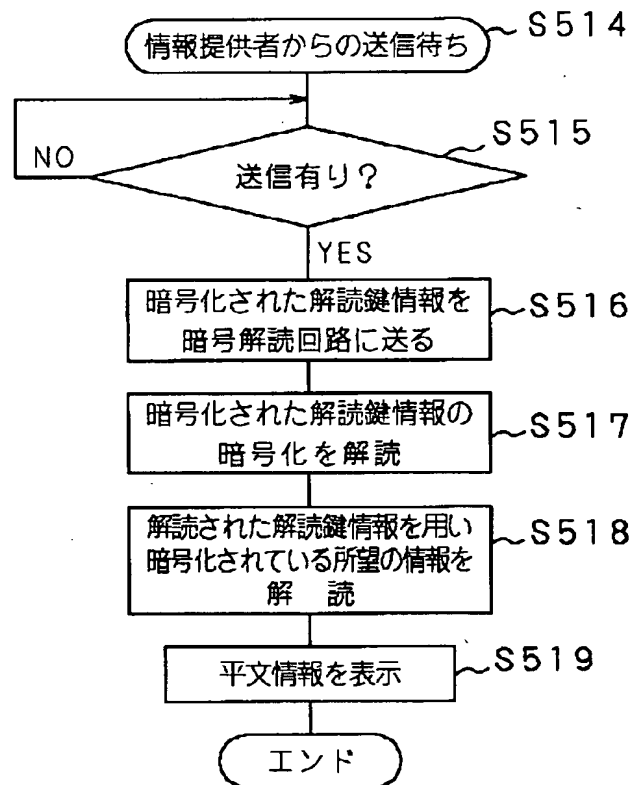
【図10】



【図11】



【図12】



フロントページの続き

(72)発明者 川嶋 功
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 応和 英男
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ ~~FADED~~ TEXT OR DRAWING
- ☐ ~~BLURRED~~ OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.